National Strategy for Trusted Identities in Cyberspace

Applicants' Webinar
January 31, 2014

Agenda

1:30 NSTIC Overview and Status Update

Jeremy Grant, Senior Executive Advisor for Identity Management

1:50 NSTIC Pilots Cooperative Agreement Program – Purpose and Scope

Jeremy Grant, Senior Executive Advisor for Identity Management

2:20 Overview of the Pilot Projects Federal Funding Opportunity

Michael Garcia, Deputy Director, NSTIC

2:50 Administrative Requirements

Dean Iwasaki, NIST Grants Specialist

3:10 Questions and Answers

Jeremy Grant, Senior Executive Advisor for Identity Management

National Strategy for Trusted Identities in Cyberspace

Jeremy Grant

Senior Executive Advisor, Identity Management

National Institute of Standards and Technology (NIST)

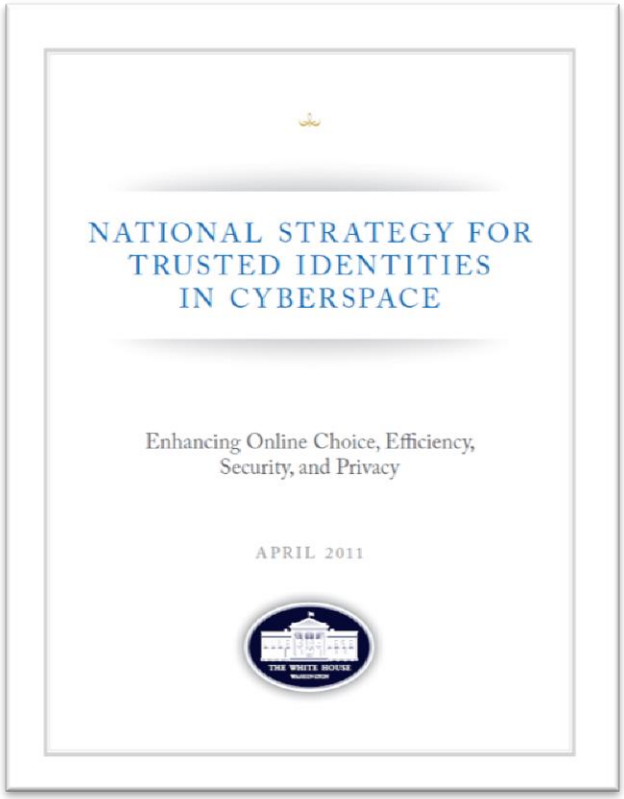
What is NSTIC?

Called for in President's Cyberspace Policy Review (May 2009):
a "cybersecurity focused identity management vision and strategy…that addresses privacy and civil-liberties interests, leveraging privacy-enhancing technologies for the nation."

Guiding Principles

- Privacy-Enhancing and Voluntary
- Secure and Resilient
- Interoperable
- Cost-Effective and Easy To Use

NSTIC calls for an **Identity Ecosystem**,
"an online environment where individuals and organizations will be able to trust each other because they follow agreed upon standards to obtain and authenticate their digital identities."



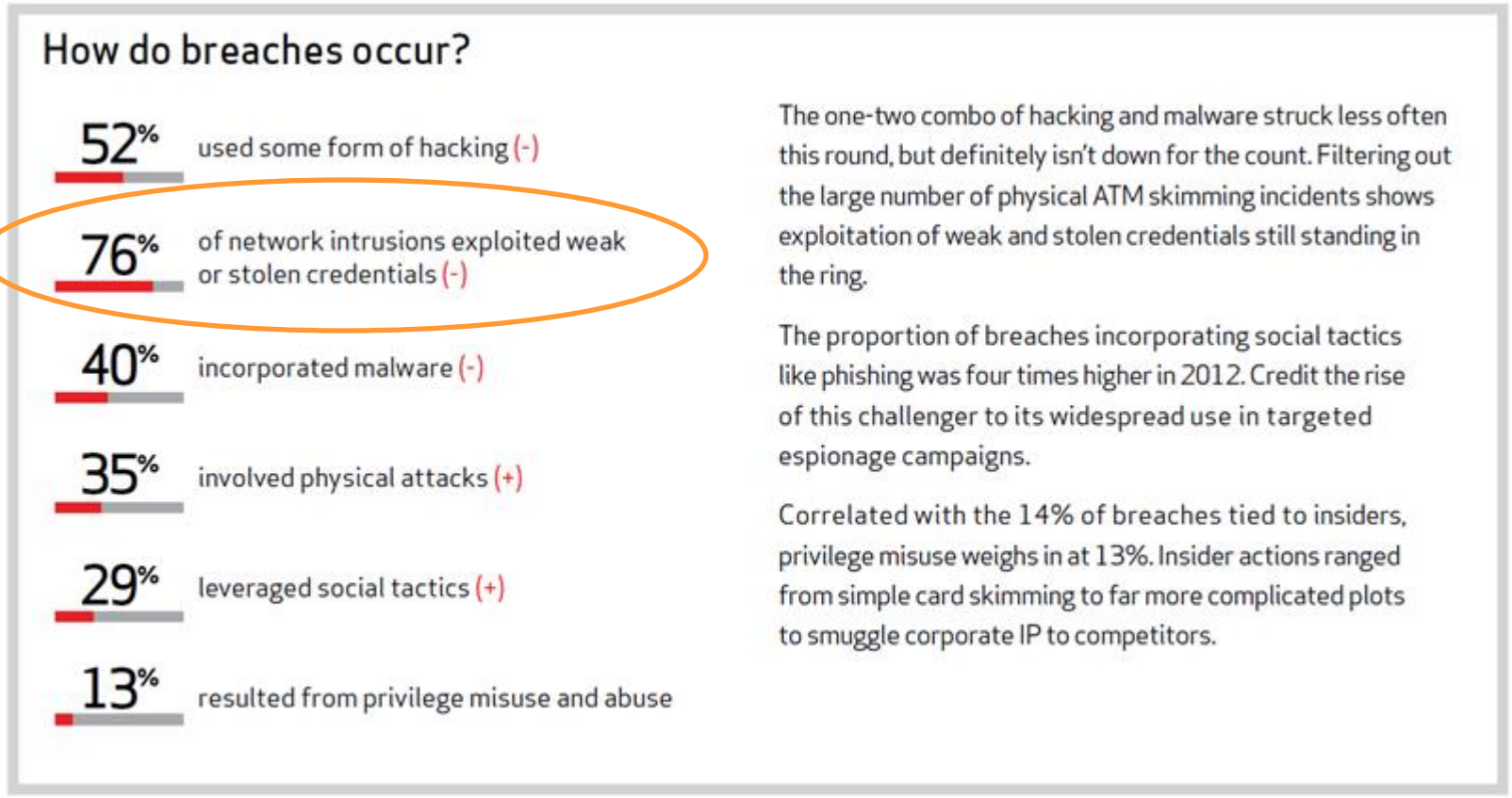
The Problem Today

Usernames and passwords are broken

- Most people have 25 different passwords, or use the same one over and over
- Even strong passwords are vulnerable…criminals have many paths to easily capture "keys to the kingdom"
- Rising costs of identity theft
  - **16.6M** U.S. victims (+43% YoY) in 2012 at a cost of **$24.7 billion**
  - **48% increase** in # of **data breaches in 2012**

    (Source: Javelin Strategy & Research)
- A common vector of attack
  - Sony Playstation, Zappos, LinkedIn, Twitter, Evernote among dozens of recent breaches tied to passwords.

The password is very much alive



Source: 2013 Data Breach Investigations Report, Verizon and US Secret Service

The Problem Today

Table 7. Top 10 Threat Action Types by number of breaches and records

Rank	Variety	Category	Breaches	Records
1	Keylogger/Form-grabber/Spyware (capture data from user activity)	Malware	48%	35%
2	Exploitation of default or guessable credentials	Hacking	44%	1%
3	Use of stolen login credentials	Hacking	32%	82%
4	Send data to external site/entity	Malware	30%	<1%
5	Brute force and dictionary attacks	Hacking	23%	<1%
6	Backdoor (allows remote access/control)	Malware	20%	49%
7	Exploitation of backdoor or command and control channel	Hacking	20%	49%
8	Disable or interfere with security controls	Malware	18%	<1%
9	Tampering	Physical	10%	<1%
10	Exploitation of insufficient authentication (e.g., no login required)	Hacking	5%	<1%

2011: **5 of the top 6** attack vectors are tied to passwords

2010: **4 of the top 10**

Source: 2012 Data Breach Investigations Report, Verizon and USSS

Passwords are bad for business

- 75% of customers will avoid creating new accounts. 54% leave the site or do not return when asked to create a new password

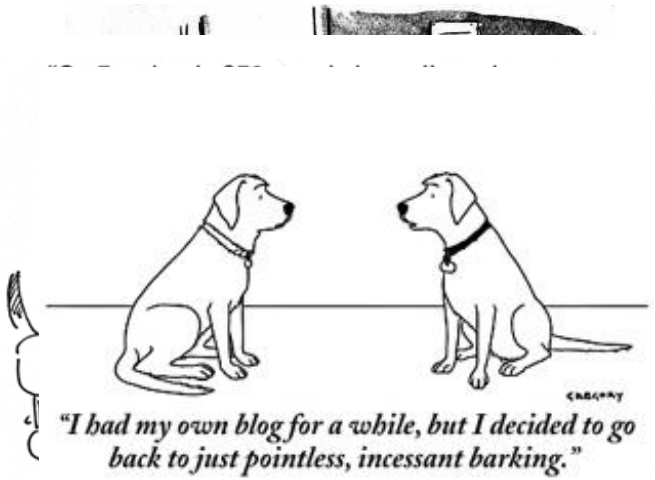
- 45% of consumers will abandon a site rather than attempt to reset their passwords or answer security questions

The Problem Today

Identities are difficult to verify over the internet

- Numerous government services still must be conducted in person or by mail, leading to continual rising costs for state, local and federal governments

- Electronic health records could save billions, but can't move forward without solving authentication challenge for providers and individuals



New Yorker, July 25, 2005

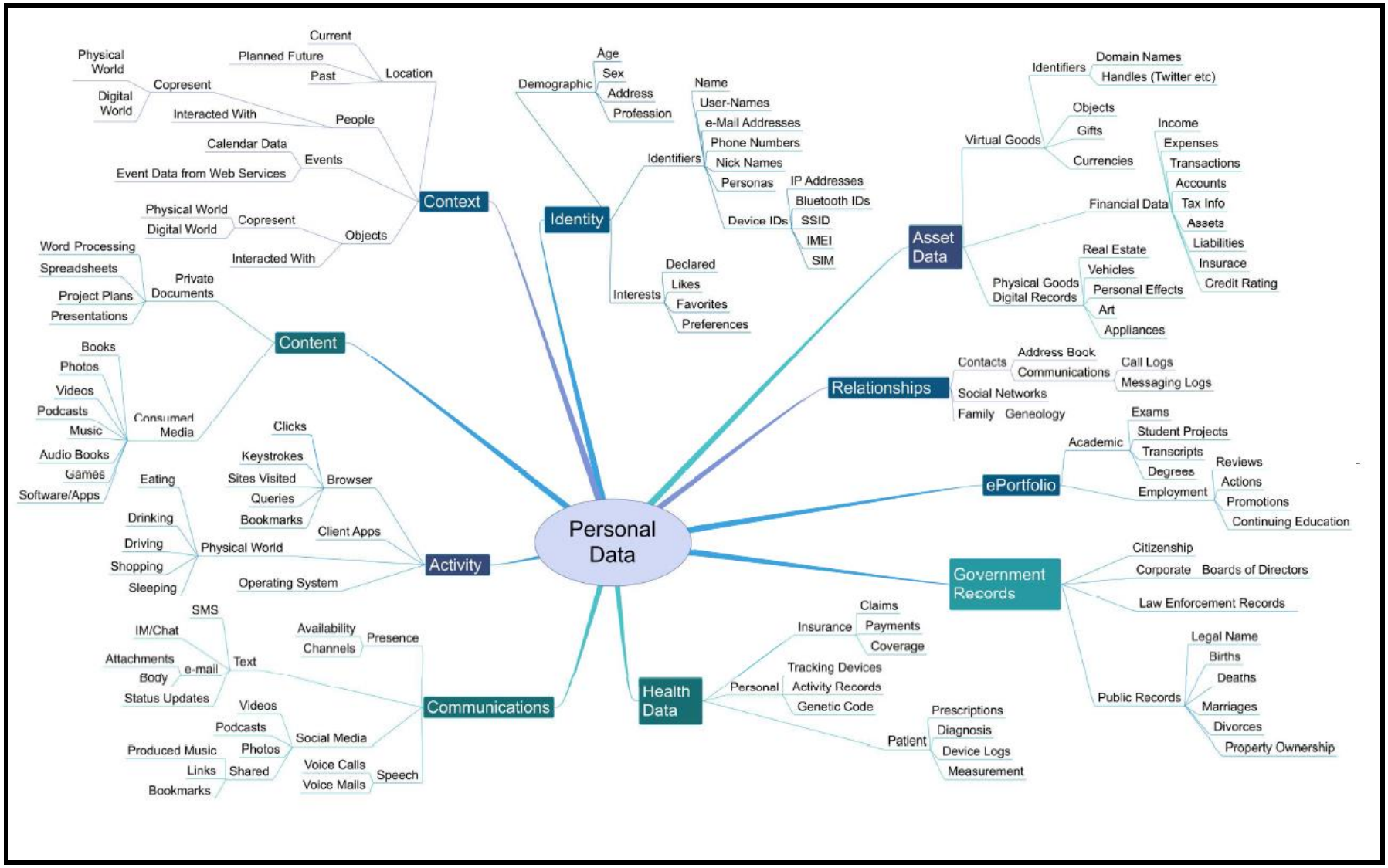
- Many transactions, such as signing an auto loan or a mortgage, are still considered too risky to conduct online due to liability risks

The Problem Today

Privacy remains a challenge

- Individuals often must provide more personally identifiable information (PII) than necessary for a particular transaction
  - This data is often stored, creating “honey pots” of information for cybercriminals to pursue
- Individuals have few practical means to control use of their information

Privacy: Increasingly Complex as Volumes of Personal Data Grow



Source: World Economic Forum, *"Rethinking Personal Data: Strengthening Trust,"* May 2012

Trust matters to online business

$2 Trillion

The total projected online retail sales across the G20 nations in 2016

$2.5 trillion

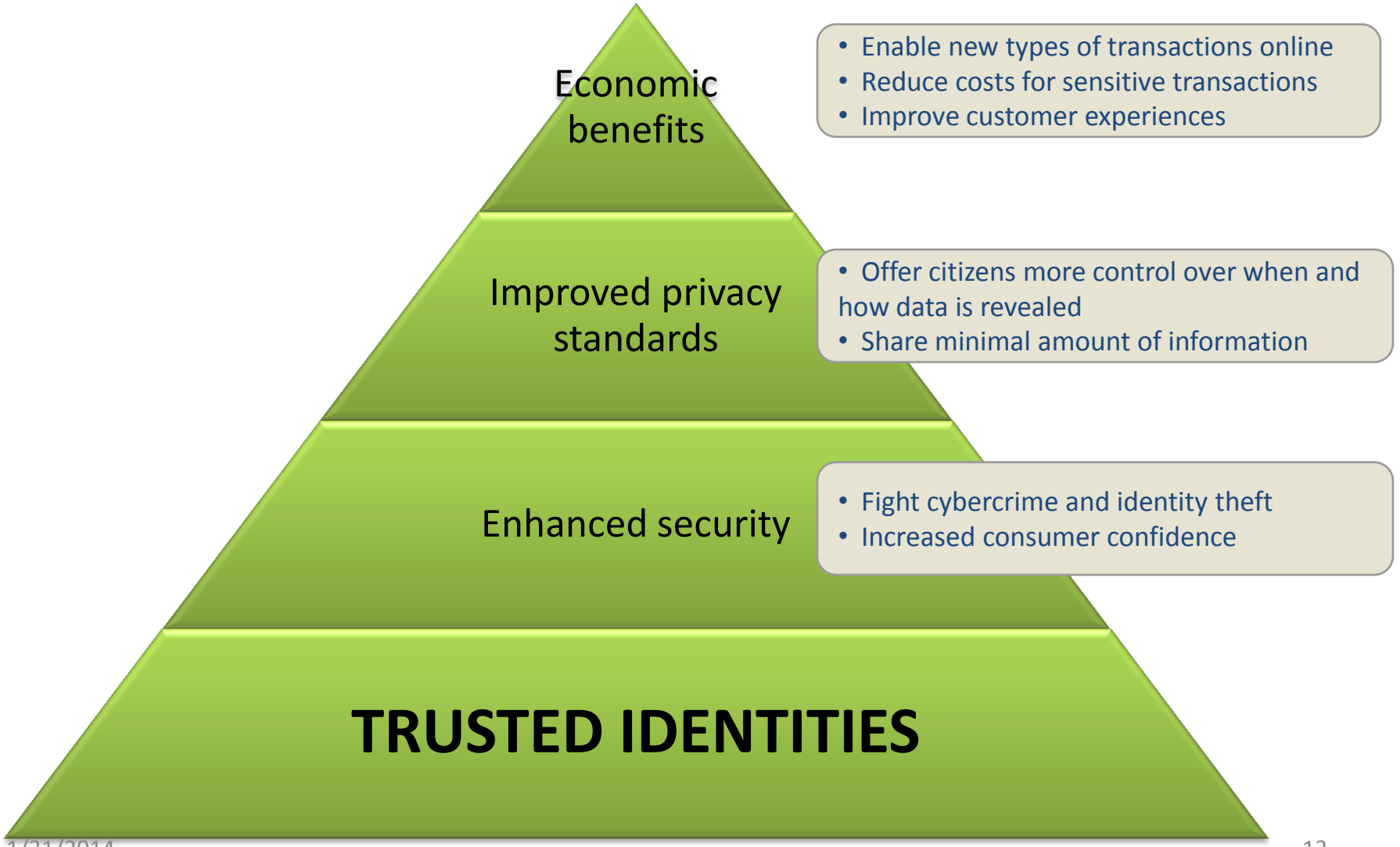
What this number can grow to if consumers believe the Internet is more worthy of their trust

$1.5 Trillion

What this number will fall to if Trust is eroded

Source: *Rethinking Personal Data: Strengthening Trust*. World Economic Forum, May 2012.

Trusted Identities provide a foundation



January 1, 2016

The Identity Ecosystem: Individuals can choose among multiple identity providers and digital credentials for convenient, secure, and privacy-enhancing transactions anywhere, anytime.

Apply for mortgage online with e-signature

Online shopping with minimal sharing of PII

Trustworthy critical service delivery

Secure Sign-On to state website

Security ‘built-into’ system to reduce user error

Privately post location to her friends

We've proven that Trusted Identities matter

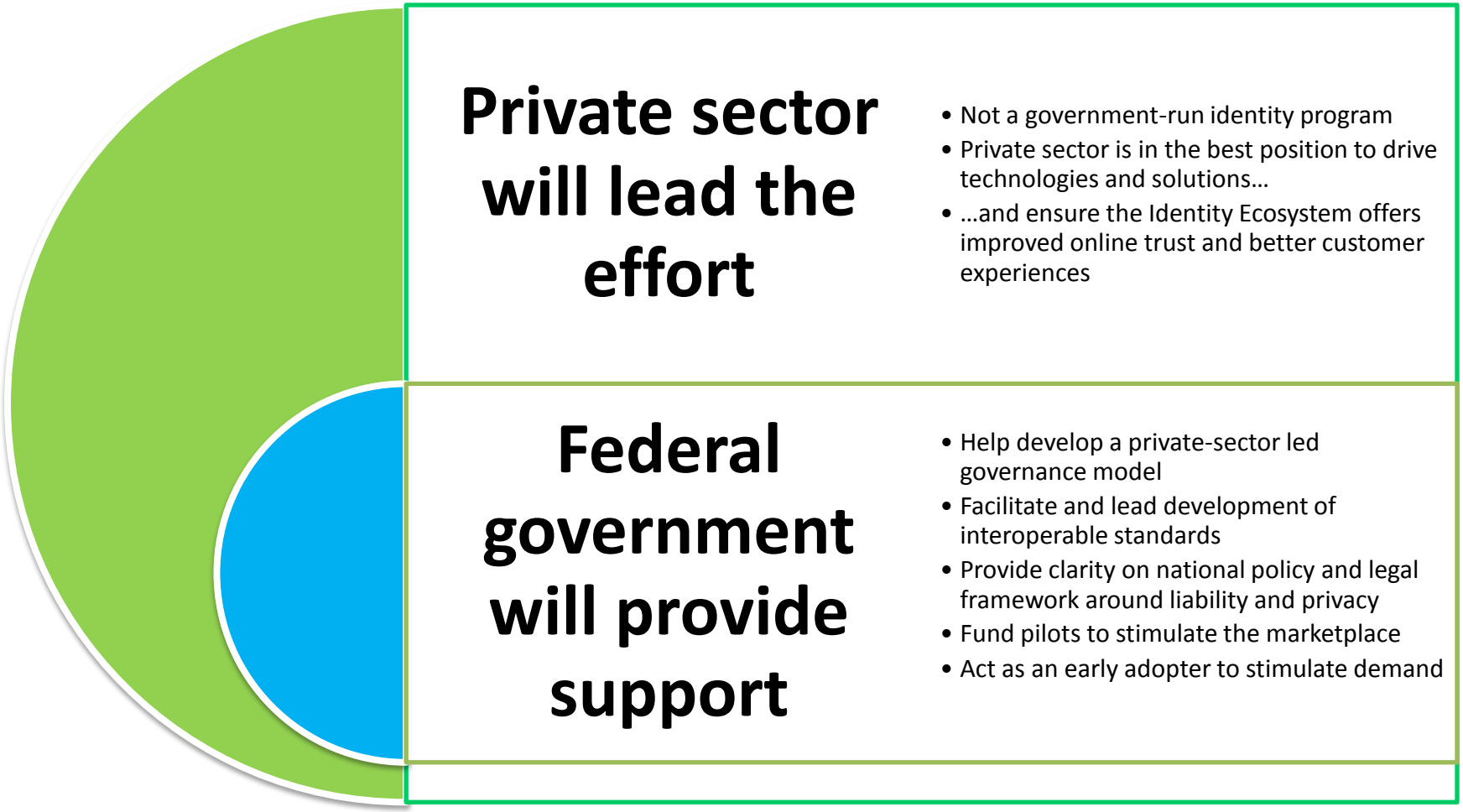
DoD Led the Way

- DoD network intrusions fell 46% after it banned passwords for log-on and instead mandated use of the CAC with PKI.

But Barriers Exist

- High assurance credentials come with higher costs and burdens
- They've been impractical for many organizations, and most single-use applications.
- Metcalfe's Law applies – but there are barriers (standards, liability, usability) today that the market has struggled to overcome.

What does NSTIC call for?



NSTIC National Program Office (NPO)

- Charged with leading day-to-day coordination across government and the private sector in implementing NSTIC
- Steady funding at $16.5M in FY12, FY13 and FY14.

Key Implementation Steps

Convene the Private Sector

- August 2012: Launched privately-led **Identity Ecosystem Steering Group (IDESG).** Funded by NIST grant, IDESG tasked with crafting standards and policies for the Identity Ecosystem Framework http://www.idecosystem.org/
- October 2013: IDESG incorporates as 501(c)3, prepares to raise private funds

Continued Support for Pilots

- **5 pilots totaling $9.2M** awarded September 2012
- **5 pilots totaling $7.4M** awarded September 2013
- **2 pilots for state benefits programs totaling $2M** awarded Sept. 2013
- Challenge-based approach focused on addressing remaining barriers
- New FFO for 2014 pilots out now

Government as an early adopter to stimulate demand

- Ensure government-wide alignment with the Federal Identity, Credential, and Access Management (FICAM) Roadmap
- New White House initiated effort to create a **Federal Cloud Credential Exchange** (FCCX)
- August 2013: **USPS** awards FCCX contract

National Strategy for Trusted Identities in Cyberspace

Pilots Program – Purpose and Scope

Jeremy Grant

Senior Executive Advisor, Identity Management

National Institute of Standards and Technology (NIST)

Pilot Overview

Purpose

- Advance the NSTIC vision, objectives, and guiding principles.
- Demonstrate innovative frameworks that can provide a foundation for the Identity Ecosystem, and tackle barriers that have, to date, impeded the Identity Ecosystem from being fully realized.

Pilot Overview

"Make something happen that otherwise would not"

- Pilots should test or demonstrate new solutions, models or frameworks that do not exist or are not widely adopted in the marketplace today…
- … and that would be unlikely to be widely adopted in a timely manner – at least in a way that supports NSTIC – without this pilot funding

Focus on Barriers

Identity solutions marketplace has struggled, in part, due to a number of barriers that market forces alone have been unable to overcome. These barriers include, but are not limited to:

- A dearth of identity solutions and trust frameworks that cross multiple sectors – making it difficult for the benefits of successful identity solutions in one sector to be realized across others.
- A lack of common standards for security, privacy, performance benchmarking and data use.
- The dissonance arising from rapidly changing technology and its impact on individual privacy and civil liberties.
- Lack of clarity on liability and other complex economic issues (e.g., "who is liable if something goes wrong in a transaction?" "How – if at all – should transactions be monetized?").
- A lack of commonly accepted technical standards to ensure interoperability among different authentication solutions.
- Challenges with usability of some strong authentication technologies.
- Challenges with balancing transparency to individual users with ease of use.

Focus on Barriers

- Pilots provide creative solutions to overcoming barriers.
- Pilots demonstrate the feasibility of solutions consistent with the NSTIC vision and guiding principles.
- Pilots provide foundation upon which Identity Ecosystem can be constructed
- Pilots help the Identity Ecosystem Steering Group (IDESG) by bringing actual implementation results to augment theoretical discussions

A Challenge-based Approach

- FFO lays out 10 objectives that are “challenges” for applicants to solve.

- Applicants are not limited to addressing these 10 challenges– there are certainly other notable challenges worthy of attention.

- 10 objectives provide a starting point for applicants to consider.

Examples

1. Demonstrate the feasibility of the Identity Ecosystem, via projects that interoperably and securely link multiple sectors via trust frameworks, including multiple identity providers (IDPs) and relying parties (RPs).

2. Expand the acceptance and use of trust frameworks and third-party credential providers by RPs.

Examples

3. Create and demonstrate solutions that can help public and private sector entities alike more easily jumpstart adoption of trusted strong authentication technologies in lieu of passwords at public-facing websites. For example, secure and reliable identity exchange hubs that can quickly validate and process strong credentials across multiple trust frameworks, while enabling enhanced privacy and civil liberties protections.

Examples

4. Create user-centric solutions to address the limitations and barriers that have inhibited consumer demand for strong authentication technologies and incentivize consumers to obtain a strong credential. For example, demonstrate how advances in usability and accessibility can improve user comfort with and uptake of strong authentication technologies.

Examples

5. Create and demonstrate a framework of policies, rules of behavior, and agreements among Identity Ecosystem stakeholders that can be applied across multiple trust frameworks and provides:
   a. Increased certainty on liability and other economic issues
   b. a strong set of privacy and civil liberties protections for all Identity Ecosystem participants, focused on fully addressing the issues outlined in Objective 1.1 of NSTIC, "Establish improved privacy protection mechanisms"
   c. A means for establishing and implementing quantifiable and reproducible levels of assurance for credentials

Examples

6. Demonstrate privacy-enhancing technologies that mitigate privacy and civil liberties risks – such as increased tracking and personal data aggregation – and can also support viable business models, current security requirements, and generally accepted performance standards.

7. Demonstrate interoperability across multiple solution stacks (i.e., smart cards, one time passwords, other technologies) in an identity ecosystem.

Examples

8. Create and demonstrate frameworks, methodologies, or solutions for enabling the exchange of specific attributes associated with identities while minimizing the sharing of non-essential information.

9. Demonstrate innovative approaches to usability and providing end-user transparency.

10. Demonstrate the role that public sector entities can play in helping individuals prove their identity to private sector credential providers and/or RPs.

Funding

- Up to $6 million may be made available in FY 2014
- New awards are expected to range from approximately $1,250,000 to $2,000,000 per year each with project performance periods of up to two (2) years
- Initial funding only provided for first year

Funding

A note on the ranges:

- With regard to the $1.25-2M range: applicants may request smaller or larger amounts – the range above is simply what we forecast.

- Number of awards will be contingent on available funding

- Two years is the maximum we would consider for a period of performance – entities who can demonstrate meaningful outcomes in a shorter timeframe should propose to do so.

National Strategy for Trusted Identities in Cyberspace

Overview of the Federal Funding Opportunity

Michael Garcia

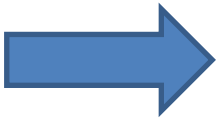
Deputy Director, NSTIC

Contents

- Eligibility
- Cost-Share
- Application Submission
- Due Dates and Timeline
- Abbreviated Application Contents
- Full Application Contents
- Application Submission
- Evaluation Criteria
- Selection Factors
- Evaluation Process

Who is an eligible applicant?

- Accredited institutions of higher education
- Non-profit organizations
- Commercial organizations
- State, local, and Indian tribal governments



located in the United States and its territories

Who is not eligible to lead a project?

- Individuals
- Federal government entities
- Entities located outside U.S.

Cost-Share

- Cost-share is not required

Abbreviated Application Submission

- All applications must be submitted through Grants.gov.
  - **Verify that your registration is up to date early!**
- Hardcopy, email or faxed applications will not be accepted.
- Applications Due by 11:59 P.M. Eastern Time on Thursday, March 6, 2014.

Abbreviated Application Contents

- SF-424, Application for Federal Assistance
- Four page technical proposal addressing the criteria

Full Application Submission

- All applications must be submitted through Grants.gov.
  - **Special Instructions will be given to finalists!**
- Hardcopy, email or faxed applications will not be accepted.
- Applications Due by 11:59 P.M. Eastern Time on Tuesday, May 13, 2014.

Application Contents

- **SF-424, Application for Federal Assistance**
  - Same as for abbreviated application
- **SF-424A, Budget Information - Non-Construction Programs**
  - Budget should reflect anticipated expenses for each year of the project of no more than two (2) years, considering all potential cost increases, including cost of living adjustments.
- **SF-424B, Assurances - Non-Construction Programs**
- **CD-511, Certification Regarding Lobbying**
- **SF-LLL, Disclosure of Lobbying Activities (if applicable)**

Full Application Contents – Cont.

- **Full Technical Application**
  - Word-processed document
  - No more than twenty-five (25) pages
  - Responsive to program description and evaluation criteria
  - Contains the following:
    - Executive Summary
    - Problem Statement and Use Cases
    - Operational Pilot
    - Statement of Work and Implementation Plan
    - Project Impact
    - Qualifications
- **Budget Narrative**

Statement of Work and Implementation Plan

- Discusses the specific proposed tasks
- Includes a schedule of measurable events and milestones
- Includes measurable performance objectives
- Can include a Gantt chart, Work Breakdown Structure or other format to present plan (not included in the page count)

Letters

- Letters of commitment to participate from third parties indicating their commitment to participate and what they will do:
  - Subawardees
  - Contractors
  - Other collaborators
- Letters are outside the page count

Evaluation Criteria

- Adherence to NSTIC Guiding Principles (40 points)
  a) Privacy-enhancing and voluntary (10 points)
  b) Secure and resilient (10 points)
  c) Interoperable (10 points)
  d) Cost Effective and Easy to Use (10 points)
- Quality of Implementation Plan (30 points)
- Contribution to Identity Ecosystem (20 points)
- Resource Availability (10 points)

Adherence to NSTIC Guiding Principles - Privacy-enhancing and voluntary

The envisioned Identity Ecosystem will mitigate privacy and civil liberties risks engendered by today's online environment of identification, tracking, and personal data aggregation. Such mitigation will be grounded in conformance to the Fair Information Practice Principles (FIPPs) (*see* Appendix A of the Strategy) in order to provide multi-faceted privacy protections.

Adherence to NSTIC Guiding Principles - Privacy-enhancing and voluntary (cont.)

Reviewers will be looking for specific details on how privacy and civil liberties will be protected and how that protection will be implemented on both a technical and policy level. Implementation details can be provided in a Privacy Impact Assessment (PIA), Privacy Evaluation Matrix (PEM) and/or mapping of the pilot details to FIPPs. In particular, reviewers will be looking for a demonstrated understanding of the privacy or civil liberties risks raised by the application and the appropriateness of mitigations for such risks, including:

Adherence to NSTIC Guiding Principles - Privacy-enhancing and voluntary (cont.)

i. How the application:
   1. Addresses any collection, use, and disclosure or transmission of personal information;
   2. Addresses when and in what manner users will be provided with information about how project participants (the project lead, contractors, subawardees and other collaborators) collect, use, disseminate, and maintain personal information, as well as how individuals can control their personal information and attributes;
   3. Addresses why and for how long personal information will be retained, the appropriateness of the development of any new databases of personal information, as well as security measures for any such retention;
   4. Minimizes retention of personal information;
   5. Minimizes data aggregation and linkages across transactions;

Adherence to NSTIC Guiding Principles - Privacy-enhancing and voluntary (cont.)

i. How the application: (cont.)

6. Provides appropriate mechanisms to allow individuals to access, correct, and delete personal information;
7. Establishes accuracy standards for personal information used in identity assurance, authentication or authorization solutions;
8. Protects, transfers at the individual's request, and securely destroys personal information when terminating business operations or overall participation in the Identity Ecosystem;
9. Accounts for how personal information is actually collected, used, disclosed or transmitted and retained, and provides mechanisms for compliance, audit, and verification; and
10. Provides effective redress mechanisms for, and advocacy on behalf of, individuals who believe their personal information may have been misused.

Adherence to NSTIC Guiding Principles - Privacy-enhancing and voluntary (cont.)

ii. Identifying how FIPPs will be used to address the topics in section (i) above; whether they will be implemented by policy and/or technical measures, although policy measures should not be used to mitigate privacy or civil liberties risks created by the technical design of the project; which project participant(s) will be responsible for the implementation; and supporting performance metrics for such implementations; and

iii. Describing what role, if any, trust frameworks will play in the enforcement of a common privacy framework applicable to all project participants, including IdPs, APs, brokers and RPs.

Adherence to NSTIC Guiding Principles - Secure and Resilient

Security ensures the confidentiality, integrity and availability of identity solutions, and the non-repudiation of transactions. Credentials are resilient when they can easily and in a timely manner recover from loss, compromise, or theft and can be effectively revoked or suspended in instances of misuse. In addition to credentials, information stores also need to be protected.

Adherence to NSTIC Guiding Principles - Secure and Resilient (cont.)

Reviewers will be looking for specific details on how solutions are secure and resilient. Examples of such details may include, but are not limited to:

- How new or existing Trust Frameworks ensure all project participants adhere to appropriate, risk-based levels of security.
- How solutions embrace security mechanisms that provide material security advances over the password-based regime dominant in the marketplace today.
- How solutions will provide secure and reliable methods of electronic authentication.
- How solutions demonstrate the integration of all major aspects of the project.

Adherence to NSTIC Guiding Principles - Interoperable

Interoperability enables service providers to accept a variety of credentials and identity media and also supports identity portability enabling individuals to use a variety of credentials in asserting their digital identity to a service provider. Interoperability needs to go beyond standards conformity to address policy and procedural interoperability. Reviewers will be looking for applications that foster the reduction and elimination of policy and technology silos and adhere to open standards. Proprietary solutions that limit interoperability will be less competitive.

Adherence to NSTIC Guiding Principles - Interoperable (cont.)

Reviewers will be looking for specific details on how proposed solutions are interoperable. Examples of such details may include, but are not limited to:

- How new or existing Trust Frameworks ensure all project participants adhere to common standards, policies, and rules and ensure proper and consistent treatment of personal data.
- How solutions leverage existing standards and/or demonstrate the need for new standards and an ability to materially advance the development and adoption of new standards.
- How solutions can be used across multiple sectors and RPs.
- How individual credentials are simply and securely portable between RPs with appropriate notifications to individuals.

Adherence to NSTIC Guiding Principles - Cost-effective and Easy to Use

Identity solutions should be simple to understand, intuitive, easy-to-use, and enabled by technology that requires minimal user training. This can be achieved with the thoughtful integration of usability principles and user-centered design. Many existing technology components in widespread use today (e.g., mobile phones, smart cards, and personal computing devices) can be leveraged to act as or contain a credential.

Adherence to NSTIC Guiding Principles - Cost-effective and Easy to Use (cont.)

Reviewers will be looking for specific details on how solutions are cost-effective and easy to use. Examples of such details may include, but are not limited to:

- How new or existing Trust Frameworks can lower costs for all Identity Ecosystem stakeholders and erase barriers to usability.
- How solutions do not present significant usability challenges.
- How solutions propose innovative applications of technology that enhance usability, relative to current market solutions.
- How costs per user are not prohibitive and can grow the Identity Ecosystem in accordance with NSTIC's four guiding principles (*see* Section I of this FFO).
- How solutions lower barriers for user acceptance and can be easily incorporated into current user activities.
- How service level agreements provide easy to understand opt-in choices for the consumer to use a service.

Quality of Implementation Plan

Quality of the applicant's plans for implementation including details on the following: tasks, schedule, quantified objectives, milestones, metrics, method of evaluating the metrics, risks, and plans for stakeholder outreach and integration with other efforts. The implementation plans should include all project participants including relying parties' activities during the project. Measurable milestones tied to metrics need to be established throughout the project for demonstrating progress in all areas relevant to the overall pilot. Milestones should be realistic and achievable in the allotted timeframes with the proposed resources. All aspects discussed as part of the solution should be included in the implementation plan and have associated milestones. Milestones should reflect the work of all participants on the project including relying parties.

Contribution to Identity Ecosystem

Explain how the operational pilot will contribute to the Identity Ecosystem in the following areas:

- **Unique Contribution** – The contribution that this project would make to the identity ecosystem that absent NSTIC project funding would not occur.
- **Large Scale Use** – The quality, comprehensiveness, and likelihood of success of the plan to transition a successful pilot into production expanding beyond initial pilot users.
- **Contribution to the Identity Ecosystem Steering Group (IDESG)** – How the applicant intends to interact and engage with the IDESG to support the development of the Identity Ecosystem Framework.

Resource Availability

Reviewers will be looking for details on:

- The qualifications and commitment of the identified project participants including key personnel, and previously demonstrated ability to achieve positive outcomes in pilot programs and similar endeavors. A subject matter expert with specialized knowledge of privacy technology and policy issues is expected on all projects. All participating organizations are expected to identify at least one key person and that person's time commitment.
- The appropriateness of proposed resources including personnel compared to the project's scope, as well as the cost-effectiveness of the project in using available resources to complete the project.

Selection Factors

- The availability of Federal funds.
- Whether the project duplicates other projects funded by NIST, DoC, or by other Federal agencies.
- Diversity among the funded projects in successfully addressing a variety of barriers that have to date impeded the Identity Ecosystem from being fully realized.
- Diversity of technical approaches across all funded projects to providing a foundation for the Identity Ecosystem.
- Diversity in the gaps in the emerging Identity Ecosystem addressed by the funded projects.

Full Application Evaluation Process

- Administrative Review
  - Eligibility
  - Completeness
  - Responsiveness to the Scope
- Technical Review
  - Evaluation Criteria
  - At least three independent reviews
- Evaluation Panel analyzes applications and technical reviews and ranks the applications
- Selection made using rank and selection factors

National Strategy for Trusted Identities in Cyberspace

Administrative Requirements




Contents

- Budget Information
  - Contents of Budget Narrative
  - Indirect Costs
  - Allowable Costs
  - Cost Principles
  - Disallowed Costs
  - Partnering Tools – Contracts and Sub-awards
  - Cost Sharing
- Expectations under the Award
  - Payment
  - Intellectual Property
  - Reporting Requirements for Cooperative Agreements
  - Audits
- Human Subjects in Research and Software Testing

Budget Information – Contents of Budget Narrative

(a) Personnel:
- name
- job title
- role of the individual on the proposed project and work to be performed
- salary rate
- level of effort on the proposed project (in hours or percentage of time)
- total direct charges on the proposed project
- contracted personnel should be listed under the Contracts/Subawards budget category

(b) Fringe Benefits:
- identified separately from salaries and wages
- based on rates determined by organizational policy
- items included in the fringe benefit rate should not be charged under another cost category

Budget Information – Contents of Budget Narrative

(c) Travel:

- include travel to Identity Ecosystem Steering Group meetings twice a year to report progress
- for all travel, include: destination; travel dates or duration of trip; names of travelers or number of people traveling; transportation rate, lodging rate, subsistence rate (per diem); and description of how the travel is directly related to the proposed project
- for travel that is yet to be determined or a destination is not known, provide best estimates based on prior experience

Budget Information – Contents of Budget Narrative

(d) Equipment:

- property with an acquisition cost of $5,000 or more (unless the organization has established lower levels)
- expected service life of more than one year
- items that do not meet the threshold for equipment can be included under the supplies line item
- list each piece of equipment, the cost, and a description of how it will be used and why it is necessary to the successful completion of the proposed project
- allocate cost for general use equipment that is charged directly to the award according to expected usage on the project

(e) Supplies:

- provide a list of each supply, and the breakdown of the total costs by quantity or unit of cost
- describe the necessity of the cost for the completion of the proposed project

Budget Information – Contents of Budget Narrative

(f) Contracts/Subawards

- treat each contract or subaward as a separate item
- describe the services provided
- describe the necessity of the subaward or contract to the successful performance of the proposed project
- subaward costs must be fully itemized with applicable cost computations and written justification that supports the necessity of each cost

(g) Other Direct Costs

- for costs that do not easily fit into the other cost categories
- list the cost, and the breakdown of the total costs by quantity or unit of cost
- include the necessity of the cost for the completion of the proposed project

Budget Information
Indirect Costs

- Indirect costs with an approved indirect cost rate agreement are allowable costs
- Indirect cost rate agreement must be with the recipient's cognizant Federal agency
- For applicants without an negotiated rate, use the best estimate for rate to be negotiated with the DOC
- For the DoC General Indirect Cost Rate Program Guidelines for Grantee Organizations, July 2013, email Dean Iwasaki, NIST Grants Specialist, at dean.iwasaki@nist.gov

Allowable Costs

Reasonable

Allocable

Allowable under grant terms, regulations, Cost Principles, statute

Necessary for the performance of the award

Consistently charged regardless of source of funds

Budget Information - Cost Principles

- 48 CFR Part 31 (For-profits) – http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&tpl=/ecfrbrowse/Title48/48cfr31_main_02.tpl

- 2 CFR Part 220 - Educational Institutions (OMB Circular A-21) - http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&tpl=/ecfrbrowse/Title02/2cfr220_main_02.tpl

- 2 CFR Part 225 - State and Local Governments - http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&tpl=/ecfrbrowse/Title02/2cfr225_main_02.tpl

- 2 CFR Part 230 - Non-profits (OMB Circular A-122) - http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&tpl=/ecfrbrowse/Title02/2cfr230_main_02.tpl

Budget Information
Allowable Costs - examples

- Direct Costs of the Technical Work
  - Salaries of technical personnel on the project
  - Equipment used on the project (pro-rated)
  - Materials and supplies

- Travel to Identity Ecosystem Steering Group Meetings to report on the project

- Companies – audits will be required by an external auditor (CPA or cognizant Federal audit agency), as specified in the Special Award Condition in the Award Notice.

- If a recipient has never received Federal funding from any Federal agency, a certification may be required from a CPA to determine whether the recipient has a functioning financial management system meeting the provisions of 15 C.F.R. § 14.21.

Budget Information
Disallowed Costs - examples

- Profit and Fees
- Application Writing/Development
- Contingency Fees
- Any cost disallowed by the cost principles
- Any cost not required for the technical work proposed on the grant

Partnering Tools

- Vendor/Procurement
  - Principal purpose of the relationship is the acquisition, by purchase, lease, or barter, of property or services (DoC Grants Manual)

- Sub-awards
  - An award of financial assistance made under an award by a recipient to an eligible sub-recipient or by a sub-recipient to a lower sub-recipient (DoC Grants Manual)

Sub-Recipient vs. Vendor

Sub-recipient

- Performs substantive portion of the programmatic work
- Involved in the design and conduct of the project
- Usually on cost-reimbursement
- Flow-through of OMB/CFR and award requirements
- No fee or profit can be charged on the grant for subrecipients

Vendor

- Provides the goods and services within normal business operations
- Provides similar goods or services to many different purchasers
- Operates in a competitive environment
- Not subject to Federal programmatic compliance requirements
- Profit can be charged

The primary distinction between sub-recipient and vendor is the performance of programmatic work. A grantee can enter into a sub-recipient relationship using "contract" mechanism. Sub-recipient budgets are required for an award to be issued.

Cost Sharing

- Cost sharing is not required;
- For projects that propose voluntary uncommitted cost share, make clear in your application, what tasks are within the scope of the project that will be funded using Federal funds; what tasks will occur concurrently using other sources of funds; and what tasks will occur in the future once the project is complete;
- While you can include a general estimate of voluntary uncommitted cost share, the budget should include only the Federal share of the project.
- Budgets and scope are subject to negotiation and amendment, if selected for funding

Expectations and Requirements

- Administrative Requirements - 15 CFR Part 14, Uniform Administrative Requirements for Grants and Cooperative Agreements with Institutions Of Higher Education, Hospitals, Other Non-Profit, and Commercial Organizations - http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=3dd74c477a3314a30e1d8c581b93db16&rgn=div5&view=text&node=15:1.1.1.1.19&idno=15
- DoC Financial Assistance Standard Terms and Conditions, January 2013 - http://www.osec.doc.gov/oam/grants_management/policy/documents/DOC_Standard_Terms_and_Conditions_01_10_2013.pdf
- Financial Assistance Award Form - http://ocio.os.doc.gov/s/groups/public/@doc/@os/@ocio/@oitpp/documents/content/dev01_002513.pdf
- Special Award Conditions specific to NSTIC and specific cooperative agreement

Payment

- All awards are paid electronically through the Automated Standard Application for Payment (ASAP) system managed by the US Treasury
- Will be required to enroll if not already

Payment – For New Grantees

Institutions with no prior history of receiving Department of Commerce awards will be required to

- Furnish a copy of an audited financial statement.
- Obtain an Accounting System Certification. If applicable, a sample certification will be provided by NIST upon award.

Reporting Requirements

- **Financial Reports -** SF-425, Federal Financial Report in triplicate each calendar quarter, and a final SF-425 within 90-days after the end of the award
- **Performance (Technical) Reports -** a technical progress report in triplicate each calendar quarter, and a final technical progress report within 90-days after the end of the award
- **Patent and Property Reports -** as required the recipient may need to submit property and patent reports (patent reports use iEdison.gov)
- **Reporting progress to NSTIC Steering Group twice a year**

Audits

States, Local Governments, Non-Profits follow A-133
Consistent with OMB Circular A-133, "*Audits of States, Local Governments, and Non-Profit Organizations*," and the related *Compliance Supplement* - *http://www.whitehouse.gov/sites/default/files/omb/assets/a133/a133_revised_2007.pdf*

Commercial Organizations follow the audit requirements in the award terms.

Recipients should budget for audit costs as needed

Intellectual Property

- Covered by "Department of Commerce Financial Assistance Standard Terms and Conditions"
- Follows Bayh-Dole Act
- "The recipient has the right to own any invention it makes … The recipient may not assign its rights to a third party without the permission of DOC unless it is to a patent management organization (i.e., a university's Research Foundation.) The recipient's ownership rights are subject to the Government's nonexclusive paid-up license and other rights." (DoC, Financial Assistance Standard Terms and Conditions, Term L.04)

http://www.osec.doc.gov/oam/grants_management/policy/documents/DOC_Standard_Terms_and_Conditions_01_10_2013.pdf

Human Subjects - Definitions

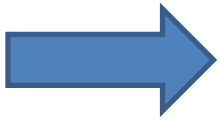
- *Human subject* - a living individual about whom an investigator conducting research obtains (1) data through intervention or interaction with the individual or (2) identifiable private information

- *Research* as a systematic investigation, including research, development, testing and evaluation, designed to develop or contribute to generalizable knowledge

  – From "The Federal Policy for the Protection of Human Subjects (the Common Rule), adopted by the Department of Commerce (DOC) at 15 C.F.R. Part 27

Human Subjects in Research- Some Key Characteristics

- Is the data provided from a commercial source?
- Is the data to be used pre-existing?
- Was the data collected for this specific project or for other purposes?
- Is the data anonymous?
- Does any of the data come from individuals who may need special protection (i.e., children)?
- Does the data involve public behavior?



Answers to these questions help NIST determine how to proceed with the approval process for the research involving human subjects.

Human Subjects in Research Examples

Uses of human subjects in research can include (but are not limited to):

- Use of existing data sets collected from individuals for testing purposes
- Collecting biometric data for testing purposes
- Surveys or focus group discussions for requirements solicitation
- Bringing in members of the user community for software testing

Statement of Work in Full Applications Should Identify Human Subjects

- Separate and identify tasks
  - that are research tasks involving human subjects
  - that are non-research tasks such as routine commercial implementation and deployment using standard procedures.

- Explain the categorization of each task

- Note that research tasks are not required in the pilots

- Human Subjects categorizations are not scored as part of the application

See OHRP Decision charts to assist in categorizing HS tasks:
http://www.hhs.gov/ohrp/policy/checklists/decisioncharts.html#c1

Documentation to Support Categorization

- If an activity/task involves data obtained through intervention or interaction with living individuals or identifiable private information obtained from or about living individuals but the project participant believes that the task/activity is not research as defined under the Common Rule, the following may be required for that activity/task:
  - Justification, including the rationale for the determination, and in some cases additional documentation to support a determination that the activity/task in the project is not research as defined under the Common Rule [see 15 C.F.R. 27.102].

Approvals for the Use of Human Subjects in Research

- NIST reserves the right to make an independent determination of whether an applicant's research involves human subjects.
- If NIST determines that a project involves human research subjects, the applicant will be required to provide additional information in writing about that part of the application for review and approval.
- If an award is issued, no research activities involving human subjects shall be initiated or costs incurred under the award until the NIST Grants Officer issues written approval.
- Retroactive approvals are not permitted.

Institutional Review Boards (IRB)

- Registered with the Office of Human Research Protections of the Department of Health and Human Services

- Information regarding how to register an IRB with OHRP and obtain a Federal Wide Assurance (FWA) for the use of human subjects can be found at http://www.hhs.gov/ohrp/assurances/index.html.

Human Subjects in Research Approval Process

Research for which Institutional Review Board (IRB) approval is required

- Must have copy of the protocol that has been (or will be) submitted to the IRB

- Applicant must have or work with an IRB that is registered with the Office of Human Research Subjects Protections (OHRP) of DHHS

- Applicant must have a Federal Wide Assurance from OHRP

Human Subjects in Research - Approval Process Continued

Research using human subjects or data from human subjects for which Institutional Review Board (IRB) approval may not be required (note: if an applicant has an IRB, the IRB will need to make a determination)

- Generally pre-existing anonymous data
- NIST will seek detailed written information on the use of human subjects or data from human subjects
- NIST will make an independent determination on what documentation is required for approval